Daily Open Source Infrastructure Report
23 July 2015

Top Stories

- U.S. and Israeli authorities arrested 4 suspects in Florida and Israel July 21 in connection to an illegal Bitcoin money laundering operation, a pump-and-dump securities manipulation scheme, and a 2014 cyberattack on JPMorgan Chase that compromised the information of 83 million customers. – *New York Times* (See item **2**)
- The Institute for Critical Infrastructure Technology released a report citing the lack of a comprehensive governing policy as the greatest failure leading to the June U.S. Office of Personnel Management systems breach, among other findings. – *Nextgov* (See item **13**)
- Google released an update for Chrome addressing 43 security vulnerabilities that could be leveraged to take control of an affected system. – *Help Net Security* (See item **18**)
- A 5-alarm fire shut down nearby roadways July 22 and severely damaged a North Brunswick, New Jersey warehouse holding 8 businesses, and displaced residents from 6 nearby apartment buildings. – *WNBC 4 New York City* (See item **20**)

Fast Jump Menu

Energy Sector

1. *July 21, Joliet Herald-News* – (Illinois) **Police: man emptied fuel tanks at Wesley Township Highway Department.** A man was arrested July 19 after allegedly stealing over 300 gallons of diesel valued at $2,000 from a fuel tank outside the Wesley Township garage in Wilmington, Illinois.
Source: http://www.theherald-news.com/2015/07/21/police-man-emptied-fuel-tanks-at-wesley-township-highway-department/aitdwt5/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

See item **12**

Financial Services Sector

2. *July 22, New York Times* – (International) **4 arrested in schemes said to be tied to JPMorgan Chase breach.** U.S. and Israeli law enforcement officials arrested 4 suspects in Florida and Israel July 21 and are searching for another in connection to an illegal Bitcoin money laundering operation and a separate pump-and-dump securities manipulation scheme that allegedly netted millions of dollars, which the suspects allegedly funneled through international shell companies. Authorities are investigating the suspects' potential roles in a 2014 cyber-attack on JPMorgan Chase that compromised the contact information of 83 million customers.
Source: http://www.nytimes.com/2015/07/22/business/dealbook/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html?ref=dealbook

3. *July 21, Orange County Register* – (California) **'Snowbird Bandit' strikes again at Rancho Santa Margarita bank.** FBI officials reported that the suspect dubbed the "Snowbird Bandit," tied to at least 3 other area robberies since June, struck a First Citizens Bank in Santa Margarita July 21.
Source: http://www.ocregister.com/articles/snowbird-673132-bandit-bank.html

Transportation Systems Sector

4. *July 22, WLWT 5 Cincinnati* – (Indiana) **Driver killed in wrong-way Interstate 74**

crash overnight. Eastbound Interstate 74 in Dearborn County was shut down for several hours July 22 while officials investigated a head-on collision that involved a semi-truck and killed one person and injured 2 others.
Source: http://www.wlwt.com/news/deadly-wrongway-crash-shuts-down-eastbound-i74/34289718

5. *July 21, Stevens Point Journal Media Journal* – (Wisconsin) **Two hurt in head-on collision in Portage County.** Highway HH and Highway J in Portage County were shut down for about 3 hours July 20 while crews responded to a head-on collision that injured 2 people. The cause of the crash remains under investigation.
Source: http://www.stevenspointjournal.com/story/news/local/2015/07/20/crash-closes-highway-hh-portage-county/30443343/

6. *July 21, Travelpulse.com* – (Florida) **Allegiant Air flight makes emergency landing in Florida.** An Allegiant Air flight from Fort Lauderdale to Memphis made an emergency landing at the Orlando-Sanford International Airport July 20 after reports of a maintenance issue and smoke in the cockpit. The 148 passengers onboard were provided replacement flights while crews investigated the cause of the smoky odor.
Source: http://www.travelpulse.com/news/impacting-travel/allegiant-air-flight-makes-emergency-landing-in-florida.html

For additional stories, see items **11** and **20**

Food and Agriculture Sector

7. *July 21, Food Safety News* – (National) **Importer recalls raw, frozen tuna linked to Salmonella outbreaks.** Osamu Corporation, a Gardena, California establishment, is recalling Frozen Yellow Fin Tuna Chunk Meat sold to AFC Corporation of Rancho Dominquez and sourced from one processing plant in Indonesia, after samples showed positive traces of Salmonella. The product was shipped to sushi restaurants nationwide.
Source: http://www.foodsafetynews.com/2015/07/importer-recalls-indonesian-raw-frozen-tuna-linked-to-salmonella-outbreaks/#.Va98HPlVhBc

Water and Wastewater Systems Sector

8. *July 22, WTAE 4 Pittsburgh* – (Pennsylvania) **25 without water, sinkhole closes road after break in Baldwin Borough.** About two-dozen Pennsylvania American Water customers in Baldwin Borough were left without water as crews worked to repair a large water main break that occurred July 21. Crews plan to have water restored by July 22.
Source: http://www.wtae.com/news/baldwin-water-main-break-closes-road-creates-sinkhole/34285212

9. *July 21, Topeka Capital-Journal* – (Kansas) **City of Topeka leak causes 55,000 gallons of raw sewage to spill into Kansas River.** Crews were working to repair and reroute the flow of the pipe after a sanitary sewer main leaked July 21 and caused 55,000 gallons of raw sewage to spill into the Kansas River in northeast Topeka. The

cause of the leak remains under investigation.
Source: http://cjonline.com/news/2015-07-21/city-topeka-leak-causes-55000-gallons-raw-sewage-spill-kansas-river \

Healthcare and Public Health Sector

10. *July 21, WTVR 6 Richmond* – (Virginia) **Power outage cancels all appointments at St. Mary's Medical Office Building South.** The Medical Office Building South at St. Mary's Hospital in Henrico, Virginia was evacuated due to excessive heat July 21 after a contractor accidentally cut power to the building.
Source: http://wtvr.com/2015/07/21/all-appointments-cancelled-at-st-marys-medical-office-building-south/

Government Facilities Sector

11. *July 22, NBC News* – (Montana) **Montana wildfires: 1,000 acres of Glacier National Park burns.** Nearly 1,000 acres of Glacier National Park were burned July 21 by the Reynolds Creek Wildland Fire, prompting evacuations of a park inn and campground. Officials said heavy timber in the area increase the risk for spreading, and a temporary flight restriction was imposed over the area.
Source: http://www.nbcnews.com/news/us-news/montana-wildfires-1-000-acres-glacier-national-park-burns-n396341

12. *July 21, Associated Press* – (Florida) **National Guard Armory evacuated in Florida after bomb report.** The National Guard Armory in Tallahassee, Florida was evacuated and several nearby buildings were placed on lockdown for 2 hours July 21 after police received a report of a suspect who claimed to have placed a bomb in the building. Nothing suspicious was found, and police are searching for the man who made the alleged threat.
Source: http://abcnews.go.com/US/wireStory/man-planted-bomb-national-guard-armory-florida-32592782

13. *July 21, Nextgov* – (National) **Security experts point to OPM's biggest cybersecurity failure.** The Institute for Critical Infrastructure Technology released a report citing the lack of a comprehensive governing policy for cybersecurity as the greatest failure leading to the June breach of its systems, and recommended that the agency address security gaps identified by auditors and implement a behavioral analytics system to compensate for rapidly advancing advanced persistent, sophisticated threats.
Source: http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-failure/118274/

Emergency Services Sector

14. *July 21, Associated Press* – (Arizona) **Ruptured cable cripples internet, 9-1-1 calls in Navajo County.** The Navajo County Sheriff reported July 21 that a Frontier Communication fiber-optic cable was cut and caused 9-1-1 call centers and emergency dispatch services to go offline from July 19 – 20. An investigation is ongoing to

determine if the cable was intentionally severed.
Source: http://www.miamiherald.com/news/business/technology/article28068859.html

Information Technology Sector

15. *July 22, Securityweek* – (International) **Siemens patches vulnerabilities in SIPROTEC, SIMATIC, RuggedCom products.** Siemens released updates for its SIPROTEC 4 and SIPROTEC Compact devices addressing a vulnerability in which an attacker could cause a denial-of-service (DoS) condition, a locally exploitable flaw in its SIMATIC WinCC Sm@rtClient application for Android in which an attacker could extract credentials for the Sm@rtServer, and a flaw in RuggedCom devices leaving them vulnerable to Padding Oracle On Downgraded Legacy Encryption (POODLE) attacks in which a man-in-the-middle (MitM) attacker could extract sensitive information from encrypted communications.
Source: http://www.securityweek.com/siemens-patches-vulnerabilities-siprotec-simatic-ruggedcom-products

16. *July 22, Help Net Security* – (International) **It's official: the average DDoS attack size is increasing.** Arbor Networks reported analysis from Quarter 2, 2015 global distributed denial-of-service (DDoS) attack data revealing that the average size of attacks increased, and that the majority of large volumetric attacks leveraged Network Time Protocol (NDP), Simple Service Discovery Protocol (SSDP), and Domain Name System (DNS) servers for reflecting amplification, among other findings.
Source: http://www.net-security.org/secworld.php?id=18651

17. *July 22, Securityweek* – (International) **Researcher discloses local privilege escalation vulnerability in OS X.** Security researchers from SektionEins released details on a vulnerability in Mac Operating System (OS) X in which an attacker could open or create arbitrary files owned by the root user anywhere in the file system by leveraging an environmental variable that enables error logging to arbitrary files.
Source: http://www.securityweek.com/researcher-discloses-local-privilege-escalation-vulnerability-os-x

18. *July 22, Help Net Security* – (International) **Google Chrome update includes 43 security fixes.** Google released an update for Chrome addressing 43 heap-buffer-overflow, use-after-free, and memory corruption vulnerabilities, among others, that could allow an attacker to take control of an affected system.
Source: http://www.net-security.org/secworld.php?id=18652

19. *July 22, IDG News Service* – (International) **Bug exposes OpenSSH servers to brute-force password guessing attacks.** Security researchers reported that OpenSSH servers with keyboard-interactive authentication enabled by default are vulnerable to unlimited authentication retries over a single connection, exposing users to brute-force password guessing attacks.
Source: http://www.networkworld.com/article/2951493/bug-exposes-openssh-servers-to-bruteforce-password-guessing-attacks.html#tk.rss_all

For another story, see item **13**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

See item **14**

Commercial Facilities Sector

20. *June 22, WNBC 4 New York City* – (New Jersey) **6 apartment buildings evacuated as warehouse inferno rages in New Jersey: officials.** A 5-alarm fire severely damaged a North Brunswick, New Jersey warehouse holding 8 businesses and displaced residents from 6 nearby apartment buildings, as well as shut down nearby roadways July 22. No injuries were reported.
Source: http://www.nbcnewyork.com/news/local/Massive-Fire-Shuts-Down-Traffic-North-Brunswick-New-Jersey-Route-1-318094581.html

21. *July 22, Staten Island Advance* – (New York) **Firefighters suffer minor injuries in blaze at Staten Island motel.** A July 22 fire at the Midland Motor Inn in Staten Island prompted the response of 33 fire units, 138 firefighters, and EMS responders to remain on site for over 2 hours to contain the incident. Four firefighters and 1 resident sustained minor injuries.
Source:
http://www.silive.com/eastshore/index.ssf/2015/07/5_injured_at_hotel_fire_in_mid.html

22. *July 22, News 12 Long Island* – (New York) **West Babylon church suffers damage after fire.** Babylon, New York officials reported July 22 that three fire departments were deployed to the St. Nicholas Greek Orthodox Church after a July 21 fire heavily damaged the facility. No injuries were reported and an investigation is ongoing to determine the cause.
Source: http://longisland.news12.com/news/west-babylon-church-suffers-damage-after-fire-1.10666086

23. *July 22, WSET 13 Lynchburg* – (Virginia) **Red Cross helps 15 people after Lynchburg apartment fire.** Lynchburg fire officials reported July 22 that 15 residents from the Jobbers Apartments were displaced after a kitchen fire activated the building's sprinkler system that damaged multiple apartment units. No injuries were reported.
Source**:** http://www.wset.com/story/29603283/red-cross-helps-15-people-after-lynchburg-apartment-fire

24. *July 21, News 13 Orlando* – (Florida) **Deltona Walmart back open after bomb threat forces evacuation.** A Walmart in Deltona, Florida was evacuated for over two hours July 21 after the store received a bomb threat that prompted the response of bomb-sniff dogs and police crews. An investigation is ongoing to determine the culprit. Source: http://www.mynews13.com/content/news/cfnews13/news/article.html/content/news/articles/cfn/2015/7/21/bomb_threat_deltona_walmart.html

25. *July 21, Associated Press* – (Washington) **Hotel fire forces 30 guests to flee room; no one injured.** Tacoma, Washington officials reported July 21 that 30 guests at the Red Lion Hotel were evacuated after a fire began in a stairwell and spread to 3 floors. No injuries were reported and officials are investigating the cause of the fire. Source: http://www.seattletimes.com/seattle-news/hotel-fire-forces-30-guests-to-flee-rooms-no-one-was-hurt/

Dams Sector

Nothing to report

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer